Washington Journal of Law, Technology & Arts

Volume 15 | Issue 3 Article 5

6-1-2020

U.S.-U.K. Executive Agreement: Case Study of Incidental Collection of Data Under the CLOUD Act

Eddie B. Kim

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 15, ISSUE 3 SPRING 2020

U.S.-UK EXECUTIVE AGREEMENT: CASE STUDY OF INCIDENTAL COLLECTION OF DATA UNDER THE CLOUD ACT

Eddie B. Kim[*]

CITE AS: E KIM, 15 WASH. J.L. TECH. & ARTS 247 (2020)
https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1308&context=wjlta

ABSTRACT

In March 2018, Congress passed the Clarifying Lawful Overseas Use of Data Act, also known as the CLOUD Act, in order to expedite the process of cross-border data transfers for the purposes of criminal investigations. The U.S. government entered into its first Executive Agreement, the main tool to achieve the goals of the statute, with the United Kingdom in October 2019. While the CLOUD Act requires the U.S. Attorney General to consider whether the foreign government counterpart has a certain level of robust data privacy laws, the relevant laws of the United Kingdom have generally been questioned numerous times for their inadequacies in protecting privacy. Thus, the privacy of U.S. citizens may be in jeopardy under the new agreement. Although the texts of the CLOUD Act and the Executive Agreement clarify that the UK government cannot explicitly target the data of U.S. citizens, it does not guarantee that such information will not be gathered incidentally. First, the UK courts do not adhere to the equivalent level of probable cause standard that is demanded under the Fourth Amendment. Therefore, they may issue judicial orders to force the U.S.-based service providers to deliver certain

[*] J.D. 2021, Columbia Law School. I am especially grateful to Professor Maeve Glass for her thoughtful comments and helpful guidance. I would also like to thank Daniel Fahrenthold and Ally Nasar as well as the entire staff at WJLTA for their input and assistance.

data, which may include information that belongs to the U.S. citizens, to the UK government upon finding mere possibility of relevance to the investigations. Coupled with this fact is arguably less robust privacy protection in the United Kingdom, from which it is not difficult to imagine a situation where the private information of U.S. citizens is extracted while the UK government seeks data belonging to citizens of its own. This Article argues that the threat to the data privacy of U.S. citizens via incidental collection is not only possible, but probable. At the same time, this Article explores possible solutions to fill in the identified gaps in the CLOUD Act that would enhance the protection of U.S. citizens' data privacy from incidental collection.

TABLE OF CONTENTS

INTRODUCTION

Since the emergence of cloud computing[1] more than a decade ago, communications service providers have been storing consumers' data on servers in different jurisdictions.[2] This is particularly a problem for law enforcement agencies when they need to extract relevant data from the service providers for the purpose of criminal investigations. For example, even if the U.S.-based service providers are under the jurisdiction of the U.S. government, for example, the data sought may be subject to the jurisdiction of another country due to the location of the server. In such cases, the agencies seeking data evidence will need to use "cross-border data access procedures" to obtain the data in question.[3] If the laws of different countries regarding disclosure of such data conflict with each other, the communication service providers "may be forced to choose which country's law to follow, knowing that they may face consequences for violating the other country's laws."[4]

---

[1] *See What is cloud computing?*, MICROSOFT AZURE, https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/ (defining cloud computing as "the delivery of computing services—including servers, or storage, databases, networking, software, analytics, and intelligence—over the internet . . . to offer faster innovation, flexible resources, and economies of scale") (last visited Feb. 9, 2020).

[2] Secil Bilgic, *Something Old, Something New, and Something Moot: The Privacy Crisis Under the CLOUD Act*, 32 HARV. J.L. & TECH. 321, 322 (2018) ("To achieve these benefits [of prevention of the loss of data due to computer crashes, less vulnerability to theft, and providing an easy medium to share files], cloud service providers move an individual's data from one jurisdiction to another . . . .").

[3] *Id*. at 323.

[4] U.S. DEP'T OF JUST., WHITE PAPER ON PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT, at 3 (2019), https://www.justice.gov/dag/page/file/1153436/download.

One of the main methods of data transfer for criminal investigation purposes is the Mutual Legal Assistance Treaty (MLAT). [5] However, this method has often proven to be cumbersome and time-consuming to the detriment of timely prosecution of criminals in some cases.[6] In March 2018, Congress passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in order to expedite the process of cross-border data transfer for the purposes of criminal investigations.[7] The statute attempts to achieve this by providing a legal basis for bilateral agreements between the U.S. government and a foreign government, which would allow for transfer of data while bypassing the requirements under an MLAT.

Since the enactment of the CLOUD Act, scholars have focused on many aspects and potential effects of the statute: practical implementation of the statute in a world where data fragmentation is prevalent,[8] data localization,[9] encryption and decryption,[10] and possible jurisdictional conflicts [11] as well as discussions on the CLOUD Act in regards to cybercrimes[12]. The statute was passed as part of an omnibus spending bill "with unusual speed and no debate."[13] Consequently, there has been much uncertainty as to how the statute will be applied in reality.[14] For example, the CLOUD Act

[5] *See infra* Section I.A.1.

[6] *See* Stephen P. Mulligan, CONG. RESEARCH SERV., R45173, CROSS-BORDER DATA SHARING UNDER THE CLOUD ACT (2018).

[7] Clarifying Lawful Overseas Use of Data Act, Consolidated Appropriations Act of 2018, Pub. L. 115-141, 132 Stat. 348, div. 5, 1213-25 (codified as amended in scattered sections of 18 U.S.C.) [hereinafter CLOUD Act].

[8] *See generally* Frederick T. Davis & Anna R. Gressel, *Feature, Storm Clouds or Silver Linings? The Impact of the U.S. CLOUD Act*, 45 LITIG. 47 (2018).

[9] *See generally* Shelli Gimelstein, *A Location-Based Test for Jurisdiction Over Data: The Consequences for Global Online Privacy*, 2018 U. ILL. J.L. TECH. & POL'Y 1 (2018).

[10] *See generally* Olivia Gonzalez, *Cracks in the Armor: Legal Approaches to Encryption*, 19 U. ILL. J.L. TECH. & POL'Y 1 (2019).

[11] *See generally* Sabrina A. Morris, *Rethinking the Extraterritorial Scope of the United States' Access to Data Stored by a Third Party*, 42 FORDHAM INT'L L.J. 183 (2018).

[12] *See generally* Chris Cook, *Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook*, 29 STAN. L. & POL'Y REV. 205 (2018).

[13] Davis & Gressel, *supra* note 8, at 48.

[14] *See generally* Dechert LLP et al., *Actual Impact of 2018 U.S. CLOUD Act*

establishes certain requirements that a foreign government must satisfy in order to be eligible to form an executive agreement with the United States under the CLOUD Act, through which data transfer may be possible for criminal investigations.[15] The statute, however, does not elaborate on how these factors—which include adequacy of laws and legal system in protecting fundamental human rights and civil rights, and against cybercrimes[16]—will come into play as the U.S. government considers a foreign government's eligibility for an executive agreement.

Indeed, privacy has also been at the heart of the conversation surrounding the new statute.[17] One of the problems flagged shortly after its enactment was the possibility of incidental collection of data under the CLOUD Act.[18] In the midst of reports from the European Data Protection Board and the Law Council of Australia indicating that the CLOUD Act would be incompatible with their equivalent laws, albeit for different reasons,[19] the U.S. government entered into its first Executive Agreement under the CLOUD Act with the United Kingdom (Executive Agreement) in October 2019.[20] In light of the newly signed Executive Agreement, this Article goes further by arguing that the threat to data privacy of U.S. citizens via incidental collection under the CLOUD Act is not only possible, but probable.

Still Hazy, JDSUPRA (July 22, 2019), https://www.jdsupra.com/legalnews/actual-impact-of-2018-u-s-cloud-act-85768/; *see also* Davis & Gressel, *supra* note 8, at 50 (stating that the CLOUD Act does not clarify whether it would apply to non-U.S. providers and that "the CLOUD Act does not fully address how these executive agreements will work in practice").

[15] *See* 18 U.S.C. § 2523(b) (2018).

[16] *See id.* § 2523(b)(1)(B).

[17] *See* Bilgic, *supra* note 2 (discussing the privacy implications of the CLOUD Act for non-U.S. citizens).

[18] David Ruiz, *A New Backdoor Around the Fourth Amendment: The CLOUD Act*, ELECTRONIC FRONTIER FOUND. (Mar. 13, 2018), https://www.eff.org/deeplinks/2018/03/new-backdoor-around-fourth-amendment-cloud-act.

[19] *See infra* Section I.C.

[20] *See* Press Release, U.S. Dep't of Just., U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online (Oct. 3, 2019), https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists.

While the CLOUD Act requires the U.S. Attorney General to consider whether the foreign government counterpart has a certain level of robust data privacy laws,[21] the relevant laws of the United Kingdom have been questioned numerous times for their inadequacies.[22] To be sure, the United Kingdom's most recent surveillance law, the Investigatory Powers Act, includes judicial oversight[23]—an addition to its previous laws struck down by the Court of Justice of the European Union and the UK courts.[24] Nonetheless, there have been doubts that the new statute actually improved the protection of data privacy of the citizens.[25] Indeed, the U.S. Attorney General has not provided justifications as to how and why the United Kingdom satisfies the requirements under the CLOUD Act.

Although the text of both the CLOUD Act and the Executive Agreement clarify that the UK government cannot explicitly target the data belonging to U.S. citizens,[26] this does not guarantee that such data will not be gathered *incidentally*.[27] The UK courts do not

---

[21] The relevant part of the statute reads:

". . . an executive agreement governing access by a foreign government to data . . . shall be considered to satisfy the requirements of this section if the Attorney General, with the concurrence of the Secretary of State, determines. . . that— (1) the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement. . ." 18 U.S.C. §2523(b)(1).

[22] *See infra* Section I.A.2.

[23] *See* Investigatory Powers Act 2016 (IPA), c. 1, § 23-25 (Eng.), http://www.legislation.gov.uk/ukpga/2016/25/contents.

[24] *See infra* Section I.A.2.

[25] *See* Scott Carey, *The Snoopers' Charter: Everything You Need to Know About the Investigatory Powers Act*, COMPUTERWORLD (July 31, 2019), https://www.computerworld.com/article/3427019/the-snoopers-charter-everything-you-need-to-know-about-the-investigatory-powers-act.html.

[26] Under the CLOUD Act, "United States person" refers to "citizens or national of the United States, an alien lawfully admitted for the permanent residence . . . or aliens lawfully admitted for permanent residence" for the purpose of the statute. 18 U.S.C. § 2523(a)(2). This Article uses the same definition when referring to "U.S. citizens."

[27] For more information regarding incidental collection in the United States, *see generally* BRENNAN CTR. FOR JUST., *Reducing "Incidental" Collection Under FISA Section 702: A Critical Protection for Americans* (Oct. 2017),

need to adhere to an equivalent standard of probable cause demanded under the Fourth Amendment in ordering the U.S.-based service providers to deliver certain data—which may include information belonging to U.S. citizens—to the UK government.[28] This may allow the UK courts to force the transfer of data upon finding mere *possibility* of relevance to the investigations. Coupled with this fact is the arguably less robust privacy protection in the United Kingdom,[29] from which it is not difficult to imagine a situation where the data of U.S. citizens is extracted while the UK government seeks data of targeted UK citizens.

To show that this potential for breach of data privacy of U.S. citizens is very real, this Article focuses on the United Kingdom's invasive surveillance regime and its use of bulk data collection in conjunction with the lack of equivalent protection of privacy provided by the Fourth Amendment. These factors may allow incidental exposure of U.S. citizens' private data to the UK government as the entity attempts to gather data of UK citizens under the Executive Agreement.

By providing background information on the CLOUD Act, Part I argues that while Congress attempted to address one problem, the thinness of the solution—the CLOUD Act and the Executive Agreement—has opened doors for other issues. Part II argues that the possibility of breach of data privacy of U.S. citizens via incidental collection is real and probable under the UK surveillance regime without any Fourth Amendment protection. To facilitate the discussion, incidental collection under the Foreign Intelligence Surveillance Act (FISA) will be discussed because of the similarities between the provisions in FISA and the CLOUD Act as well as the Executive Agreement.[30] Part III suggests recommendations that can enhance the protection of U.S. citizens' data privacy by reinforcing

---

https://www.brennancenter.org/sites/default/files/FISASection702ReducingIncidentalCollection.pdf.

[28] *See* Agreement Between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, U.K.-U.S., art. 5, Oct. 3, 2019, https://www.justice.gov/ag/page/file/1207496/download [hereinafter U.S.-UK/Ir. Executive Agreement]; *see also infra* note 132.

[29] *See infra* Section I.A.2.

[30] *See* Ruiz, *supra* note 18.

the process of evaluating potential qualifying foreign governments under the CLOUD Act and increasing the role of the communication service providers.

I. THE CLOUD ACT AND THE EXECUTIVE AGREEMENT

The inefficiencies of the current methods of cross-border data transfers and the gap in the relevant statutes—the Electronic Communications Privacy Act [31] (ECPA) and the Stored Communications Act (SCA) [32]—in terms of their extraterritorial reach are the problems the CLOUD Act purported to solve.[33] ECPA and the SCA, arguably outdated statutes, have been construed to have protection of privacy as their primary purposes, and, as discussed below, the Second Circuit ruled in accordance with that purpose in *United States v. Microsoft*.[34] This Part argues that by effectively overruling the Circuit's decision with the CLOUD Act, Congress considered data privacy to be of secondary importance compared to the facilitation of criminal investigations. And by attempting to solve the problems associated with cross-border data transfers, Congress opened doors to another problem: possibility of violation of U.S. citizens' privacy.

After briefly touching on the existing methods of transnational data transfers for criminal investigation purposes in Section I.A.1, Section I.A.2 discusses the background statutes that are in play: ECPA and the SCA. Section I.B.1 will explain the context in which extraterritorial application of the statutes became an issue before the Supreme Court in *United States v. Microsoft*,[35] to which Congress responded by passing the CLOUD Act before the Court rendered an opinion as discussed in Section I.B.2. Next, initial assessment and review of the CLOUD Act by the European Data Protection Board and the Law Council of Australia is discussed in Section I.C to

[31] 18 U.S.C. §§ 2510-23.

[32] 18 U.S.C. §§ 2701-12.

[33] *See infra* Section I.B.

[34] *See* In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 829 F.3d 197, 219-20 (2d Cir. 2016) [hereinafter *Microsoft Search Warrant Case*].

[35] 138 S. Ct. 1186 (2018).

identify potential faults in the statute. Finally, Section I.D provides an overview of relevant terms of the Executive Agreement.

A. Existing Framework for Cross-Border Data Transfers

The existing framework for cross-border data transfer for criminal investigation purposes are Mutual Legal Assistance Treaties and Letters Rogatory. The U.S. statutes that operate in the background are ECPA and the SCA. In essence, the courts consider these statutes when reviewing requests for data by other countries.

1. MLAT and Letters Rogatory

Prior to the enactment of the CLOUD Act, there were only two main (internationally established) mechanisms in which litigants in the United States could request data information located within the territorial jurisdiction of another country: the letters rogatory and the Mutual Legal Assistance process (MLA) based on MLAT.[36] One of the criticisms for both methods is that the whole procedure takes too long.[37] This is primarily due to the fact that the requests are given to the government of the receiving country—that is, the country that has jurisdiction over the location of the server holding the data in question—which will then go through additional procedures to safeguard against unlawful disclosure of private information.[38] On average, it takes approximately 10 months for the United States to respond to an MLA request.[39] Processing of the MLA requests sent

[36] In civil cases, "non-government litigants who do not have access to the MLAT process" may use letters rogatory as a method to collect evidence from another country. T. Markus Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, FED. JUD. CTR., at 17 (2014), https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf. Letters rogatory and the MLAT process is not within the scope of this Article, and, thus, their procedures will not be discussed in detail. For more detailed discussion of the two methods and their procedures, *see generally* Funk, *supra* note 36; *see also* Mulligan, *supra* note 6.

[37] *See* Mulligan, *supra* note 6.

[38] *See id*. at 12.

[39] Richard A Clarke et al., *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, at 227 (Dec. 12, 2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-

to another country by the U.S. government may take "considerably longer," if it is ever completed.[40]

2. ECPA and the SCA

In 1986, Congress enacted ECPA, "one of the primary federal laws regulating disclosure of electronic communications."[41] It protects any type of electronic communications—including emails, phone conversations, and data in general—that are made, transmitted, or stored.[42] The more relevant chapter of ECPA is Title II of the statute: the SCA. The SCA "protects the privacy of the contents of files stored by service providers and of records held by the subscriber by service providers . . . ."[43] It has been interpreted by the courts to apply to data associated with emails,[44] text messages,[45] private messages, wall postings, and other comments made on or via social media sites,[46] and even private YouTube videos.[47]

Overall, the SCA has two major components. First, unless exceptions indicated apply, the communications service providers ("CSPs")[48] are prohibited from "knowingly divulg[ing] to any

12_rg_final_report.pdf; *see also* U.S. DEP'T. OF JUST., *supra* note 4, at 2 ("Our foreign partners have long expressed concerns that the mutual legal assistance process is too cumbersome to handle their growing needs for this type of electronic evidence in a timely manner.").

[40] Mulligan, *supra* note 6, at 14.

[41] *Id*. at 3.

[42] *See* Office of Just. Programs, U.S. DEP'T. OF JUST., Electronic Communications Privacy Act of 1986, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 (Apr. 23, 2019).

[43] *Id*.

[44] *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004).

[45] *See* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 901 (9th Cir. 2008), rev'd on Fourth Amendment grounds sub nom. City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010).

[46] *See* Crispin v. Christian Audigier, 717 F. Supp. 2d 965, 980, 989 (C.D. Cal. 2010).

[47] *See* Viacom Intern. Inc. v. Youtube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008).

[48] The SCA distinguishes between a person or entity "providing an electronic communication service to the public," 18 U.S.C. § 2702(a)(1), and a person or entity "providing remote computing service to the public." 18 U.S.C. § 2702(a)(2). For the purpose of this Article, however, the difference is insignificant

person or entity the contents of a communication while in electronic storage by that service" and "contents of any communication which is carried or maintained on that service."[49] Second, the SCA requires disclosure of such data to the U.S. government, under certain circumstances when a judicial warrant is successfully obtained.[50] While the SCA has been a major tool utilized by the U.S. government to obtain electronic evidence, the statute's extraterritorial application became an issue in *United States v. Microsoft*.[51]

B. The Clarifying Lawful Overseas Use of Data Act

The extraterritorial application of the SCA became an issue when Microsoft refused to hand over certain data that were stored in Ireland which the U.S. government sought as part of a criminal investigations. Section I.B.1 briefly discusses the history behind the enactment of the CLOUD Act, which shows that Congress indeed attempted to solve the core issue in *Microsoft* but did so in haste. The result is somewhat unclear languages within the new law, hence uncertainties introduced above and further analyzed in Section I.B.2.

1. *United States v. Microsoft Corp*.

In 2016, the U.S. government, in accordance with the SCA provisions, obtained a warrant from a magistrate judge requiring Microsoft to disclose relevant contents of an email account that was allegedly used by a suspect engaged in illegal drug trafficking.[52] The

since, today, major CSPs provide both services. Thus, "CSPs" will refer to both types of providers in this Article.

[49] 18 U.S.C. § 2702(a).

[50] *See* 18 U.S.C. § 2703. The SCA requires the U.S. government to obtain a judicial warrant upon showing probable cause. *See* 18 U.S.C. § 2703(d). However, it should be noted that there are many different factors to be considered, such as when and what the government can demand when it comes to communication data from the CSPs, which will not be discussed here. For detailed discussions about which factors that must be taken into account and specific procedures to be taken for such mandatory disclosure, *see* Mulligan, *supra* note 6, at 5-6.

[51] 138 S. Ct. 1186 (2018).

[52] *Id.* at 1187.

warrant ordered Microsoft to disclose all relevant communication data "[t]o the extent that the information . . . is within [Microsoft's] possession, custody, or control." [53] While Microsoft partially complied by providing relevant data that was stored within the United States, it moved to quash the warrant with respect to the information stored in Ireland.[54] After the magistrate judge denied the motion, the District Court affirmed the ruling.[55] On appeal by the United States, the Court of Appeals for the Second Circuit reversed, holding that requiring Microsoft to disclose the electronic communications in a foreign territory would be an unauthorized extraterritorial application of § 2730 of the SCA.[56] In concluding so, the Second Circuit also emphasized that legislative history suggests that the primary purpose of their enactment was the protection of data privacy, which trumps the investigatory needs of law enforcement.[57] The Supreme Court granted writ of certiorari on October 16, 2017.[58] The case drew public attention, and numerous amici briefs were submitted by "a range of groups including privacy advocates, law enforcement officials, members of Congress, 34 U.S. states and territories, and several foreign nations."[59]

---

[53] *Id*.

[54] *See Microsoft Search Warrant Case*, at 200.

[55] *Id.* at 201.

[56] *Id.* at 222.

[57] *Id.* at 219-20 ("In enacting the SCA, Congress expressed a concern that developments in technology could erode the privacy interest that Americans traditionally enjoyed in their records and communications . . . . Accordingly, Congress set out to erect a set of statutory protections for stored electronic communications . . . . In regard to governmental access, Congress sought to ensure that the protections traditionally afforded by the Fourth Amendment extended to the electronic forum . . . . We believe this legislative history tends to confirm our view that the Act's privacy provisions were its impetus and focus. Although Congress did not overlook law enforcement needs in formulating the statute, neither were those needs the primary motivator for the enactment . . . . Taken as a whole, *the legislative history tends to confirm our view that the focus of the SCA's warrant provisions is on protecting user's privacy interests in stored communications*.") (emphasis added).

[58] Amy Howe, *Court Adds Four New Cases to Merits Docket*, SCOTUSBLOG (Oct. 16, 2017, 11:55 AM), https://www.scotusblog.com/2017/10/court-adds-four-new-cases-merits-docket/.

[59] Mulligan, *supra* note 6, at 7.

While the appeal to the Supreme Court was pending, the U.S. Department of Justice (DOJ) sought action from Congress.[60] In a hearing before the House Committee on the Judiciary in June 2017, DOJ representatives argued that the Second Circuit's decision curtailed law enforcement's ability to obtain data stored by U.S.-based CSPs abroad, which, consequently, causes harm to public safety.[61] In February 2018, a bill titled the CLOUD Act, which "revised portions of the SCA to explicitly permit the use of warrant to obtain electronic communications stored by a U.S. company on foreign servers,"[62] was introduced, passed in the House and the Senate, and signed into law by the President on March 23, 2018. Consequently, the Supreme Court rendered the *Microsoft* case moot.[63]

2. Statutory Analysis of the CLOUD Act

In April 2019, DOJ indicated that the purpose of the CLOUD Act was "to speed access to electronic information held by U.S. based global providers that is critical to our foreign partners' investigations of serious crime" wherever the data server may be located.[64] Mainly, the CLOUD Act has two critical implications. One, as mentioned above, the statute makes it explicit that the SCA will apply to content data in possession of the CSPs regardless of where the data server is located around the world.[65] DOJ clarifies,

---

[60] *See Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the digital Era: Hearing Before the H. Comm. On the Judiciary*, 115th Cong. 1 (2017) (statement of Richard W. Downing, Acting Deputy Assistant Att'y Gen., U.S. Dep't of Just.), https://docs.house.gov/meetings/JU/JU00/20170615/106117/HHRG-115-JU00-Wstate-DowningR-20170615.pdf.

[61] *Id.*

[62] Bilgic, *supra* note 2, at 332. The relevant statutory provision reads: "A [CSP] shall comply with the obligations of [the SCA] to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, *regardless of whether such communication, record, or other information is located within or outside of the United States*." 18 U.S.C. § 2713 (emphasis added).

[63] *See* United States v. Microsoft Corp., 138 S. Ct. 1186, 1188 (2018).

[64] U.S. DEP'T. OF JUST., *supra* note 4, at 2.

[65] *Id.* at 6 ("[T]he second part of the CLOUD Act clarifies that U.S. law

however, that the new "amendment . . . does not give U.S. law enforcement any *new* legal authority to acquire data . . . ."[66] Rather, the amendment simply clarifies and confirms the extraterritorial scope of the SCA.[67]

Two, the CLOUD Act authorizes the U.S. Attorney General, with the concurrence of the Secretary of State, to enter into executive bilateral agreements with other countries that would "remove restrictions under each country's laws so that the CSPs can comply with qualifying, lawful orders for electronic data issued by the other country." [68] In order to determine whether a foreign government is eligible to enter into an executive agreement with the U.S. government—or is a "qualifying foreign government" [69] (QFG)—the CLOUD Act requires that the Attorney General consider different criteria and factors, such as implementation of robust substantive and procedural laws against cybercrimes; on electronic evidence; and on protection of privacy, civil liberties, and international human rights.[70]

More relevant to this Article is the fact that a potential QFG must show commitment and respect for "international human rights, including . . . protection from arbitrary and unlawful interference with privacy" [71] and "sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data."[72] These are precisely the areas in which the previous UK surveillance regime had been questioned and failed to prevail in judicial challenges.[73] Moreover, a QFG must also have in place the procedures to "minimize the acquisition, retention, and

requires that CSPs subject to U.S. jurisdiction must disclose data that is responsive to valid U.S. legal process, regardless of where the company stores the data.").

[66] *Id*. at 8.

[67] *Id*. *See also* Mulligan, *supra* note 6, at 8 (stating that DOJ's proposal to Congress in the midst of the *Microsoft* case "was intended to restore the 'pre-*Microsoft* status quo when providers routinely complied' with the SCA warrants for data stored abroad.").

[68] U.S. DEP'T. OF JUST., *supra* note 4, at 3.

[69] Bilgic, *supra* note 2, at 336.

[70] *See* 18 U.S.C. § 2523(b).

[71] *Id.* § 2523(b)(1)(B)(iii)(I).

[72] *Id.* § 2523(b)(1)(B)(v).

[73] *See infra* Section II.A.2.

dissemination of information concerning United States persons."[74] For one, it is unclear how the United Kingdom has established such system, and, thus, satisfies this category in the eyes of the U.S. Attorney General. But even if the country has successfully put such a system in place, discussion of incidental collection under FISA, which compels the U.S. law enforcement agencies to do the same, shows that this may not be enough to protect the data privacy of U.S. citizens.[75]

There are also limitations outlined in the CLOUD Act for a QFG. In general, the statute does not create any obligation for the CSPs to decrypt any encrypted data transmitted to the QFG, or even to retain the technology to do so.[76] The CLOUD Act also amends the original text of 18 U.S.C. § 2703 by allowing the CSPs that have been issued a judicial order forcing them to hand over certain data to make Motions to Quash or Modify the court order.[77] In order to succeed in such motions in the United States, the CSPs must conjunctively establish that the targeted person is a non-U.S. person who does not reside in the United States, and that the disclosure would violate the national laws of the QFG.[78] The courts may modify or quash the motion only if that they believe that the motion should be granted in consideration of interests of justice in totality of the circumstances, in addition to finding that the CSPs have satisfied its burden of proof.[79] However, the courts may still force immediate production of requested data while the order is being challenged if the delay would cause an "adverse result identified in Section 2705(a)(2)."[80]

Other limitations are similar, if not almost identical, to provisions in FISA. For instance, the QFG may not intentionally seek or obtain data of U.S. citizens and persons located within the U.S. borders, or achieve this by targeting a foreigner located outside

---

[74] *Id.* § 2523(b)(2).

[75] *See infra* Section II.A.1.

[76] *Id.* § 2523(b)(3).

[77] *See* 18 U.S.C. § 2703(h)(2)(A).

[78] *Id.* § 2703(h)(2)(B). It should be noted that the CLOUD Act itself only seem to specify the procedures and the standards applicable in the U.S. courts but not the courts of the QFGs. *See infra* note 229.

[79] The CLOUD Act dictates that the court considering such Motion to Quash or Modify should consider international comity among other elements. *See id*. § 2703(h)(3).

[80] *Id*. § 2703(h)(4).

the United States.[81] Furthermore, the order issued by a QFG must be solely to obtain data related to a serious crime.[82] The court orders must be subject to review by an independent judicial or another authority,[83] and abide by other restrictions on wire tapping similar to those under FISA. [84] The QFG may not issue an order on behalf of the United States for data disclosure nor "be required to share any information produced with the United States Government."[85]

C. Assessment of the CLOUD Act by Foreign Authorities

While there have been many speculations on the practicality of the CLOUD Act for some time after its enactment, the European Data Protection Board (EDPB) of the European Union (EU) and the Law Council of Australia (LCA) presented clarifying views on the CLOUD Act's compatibility with their own respective equivalent laws. Simply put, the requirements under the CLOUD Act are "too hard" in comparison to the Australian law and "too soft" for the EU.[86] The compatibility assessment against the laws of the EU and Australia will be discussed for the purpose of showing the thinness of the CLOUD Act—a product of Congress' rush to answer the Second Circuit's decision in *Microsoft*.

---

[81] 18 U.S.C. § 2523(b)(4)(A), (B).

[82] *Id.* § 2523(b)(4)(D)(i).

[83] *Id.* § 2523(b)(4)(D)(v).

[84] *See id.* § 2523(b)(4)(D)(vi) ("[A]n order [issued by the QFG] for the interception of wire or electronic communications . . . shall require that the interception order . . . be for a fixed, limited duration . . . , may not last longer than is reasonably necessary to accomplish the approved purpose of the order . . . , and be issued only if the same information could not reasonably be obtained by another less intrusive method."). *Cf.* 50 U.S.C. § 1805 (specifying the requirements, as to duration, for example, to be met for a court order under FISA).

[85] *Id.* § 2523(b)(4)(C).

[86] Marcus Evans et al., *US Cloud Act and International Privacy*, NORTON ROSE FULBRIGHT: DATA PROTECTION REP. (Aug. 1, 2019), https://www.dataprotectionreport.com/2019/08/u-s-cloud-act-and-international-privacy/.

1. The European Union and the GDPR

The General Data Protection Regulation (GDPR) of the EU became binding on all member states as of May 25, 2018.[87] Written by the European Parliament and the Council of the EU, the GDPR was implemented "not only to enhance and safeguard the rights that individuals have over their data but . . . to create a simple and efficient regulatory environment, where compliance with the regulation is a key element, not only for public sector, but also for private businesses."[88]

On July 10, 2019, the EDPB and the European Data Protection Supervisor (EDPS) issued an initial assessment of the CLOUD Act in relation to the GDPR.[89] They concluded that a U.S.-based CSP active in the European market would not be able to transfer data to the U.S. government under the CLOUD Act without violating the GDPR. [90] The main obstacle, the two entities claim, is the incompatibility between the requests under the CLOUD Act and Articles 6, 48, and 49 of the GDPR.[91]

---

[87] Directive 2016/679 of the European Parliament and of the Council of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119), https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679 [hereinafter GDPR].

[88] Georgios Roussaris, *EU Policies in Data Governance: The New Challenge on the Field of Public Administration*, at 26 (2019), https://dspace.lib.uom.gr/bitstream/2159/23080/4/RoussarisGeorgiosMsc2019.pdf.; *see also Data Governance: Landscape Review*, THE ROYAL SOCIETY, at 9 (June 2017), https://royalsociety.org/~/media/policy/projects/data-governance/data-governance-landscape-review.pdf.

[89] *See* European Data Protection Board (EDPB), ANNEX. Initial Legal Assessment of the Impact of the US CLOUD Act on the EU Legal Framework for the Protection of Personal Data and the Negotiations of an EU-US Agreement on Cross-border Access to Electronic Evidence (July 10, 2019), https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf.

[90] *Id.*

[91] It should be noted that the EDPB stated that there may be certain exceptions. *See id*. n.18 ("The European Commission takes the view that some derogations under Article 49 GDPR might be used, depending on the circumstances of the case.").

First, Article 48 of the GDPR requires that a judicial or an administrative order requesting disclosure of personal data from a CSP within the EU "may only be recognized or enforceable in any manner if based on an international agreement."[92] Since executive agreements under the CLOUD Act are not treated as such international agreement by the EU,[93] the CSPs will not be able to transfer personal data to the U.S. government under the CLOUD Act without violating Article 48, unless there is "another legal basis under the GDPR."[94]

Second, Article 6(1)(c) requires that the data transfer be "necessary for compliance with a legal obligation to which the [CSP] is subject."[95] However, because "legal obligation" in this context can only have basis under the law of the EU or the Member States,[96] a CLOUD Act-based request would create legal obligations for a CSP *only if* the EU enters into a separate international agreement with the United States under Article 48.[97] Neither would such request have legal basis under Article 6(1)(e)[98] for the same reasons.[99] Additionally, although Article 6(1)(d) may allow transfer of personal data "in order to protect the vital interests of the data subject or of another natural person,"[100] the GDPR states that the transfers for the latter purpose should take place only when there is no other legal basis for doing so.[101] Consequently, while data

[92] GDPR, art. 48.

[93] While Article 48 of the GDPR explicitly states that an MLAT between the EU and another country will suffice, it seems that an executive agreement with the United States under the CLOUD Act will not be treated as an "international agreement" under Article 48. *See* EDPB, *supra* note 89, at 3.

[94] *Id*.

[95] GDPR, art. 6(1)(c).

[96] *Id.* art. 6(3).

[97] *See* EDPB, *supra* note 89, at 4.

[98] *See* GDPR, art. 6(1)(e) ("Processing shall be lawful only if . . . processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.").

[99] *See* EDPB, *supra* note 89, at 4-5 ("We consider that Article 6(1)(e) may not constitute a valid legal basis [because] where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, according to Article 6(3) GDPR, the processing should have basis in Union or Member State law.").

[100] GDPR, art. 6(1)(d).

[101] *See* GDPR, recital 46. ("Processing of personal data based on vital interest

transfer may be lawful if its purpose was to protect the vital interest of the data subject, the same cannot be said for "another natural person" because the EU-US MLAT is a valid alternative legal basis for requesting such information.[102] Lastly, data transfers may be lawful under Article 6(1)(f)[103] only if the legitimate interests of the CSPs or those of the U.S. government outweigh the interests or fundamental rights and freedoms of the data subject.[104] In evaluating the balancing test, the EDPB and the EDPS clarify that the U.S. government is "not [one of the] public or competent authorities established under EU Law," and, thus, cannot fall within the definition of "third party" for the purposes of Article 6(1)(f); the latter element of the balancing test will likely override the former due to potential violation of data subject's right to effective remedy, the principle of dual criminality, and circumstances in which the CSPs will need to act on the basis of limited information.[105]

Finally, the EDPB and the EDPS discussed whether disclosure of data under the CLOUD Act would be compatible under Article 49: Derogations for Specific Situations.[106] They answered in the negative. The legality of such transfer under Article 49(1)(d)[107] is rejected because "only public interests recognised in Union law or in the law of the Member State to which the controller is subject can lead to the application of this derogation," and that of the United States is not relevant.[108] It is conceded that data transfer *may* be lawful under Article 49(1)(e)[109] under certain circumstances.[110]

---

of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis.").

[102] *See* EDPB, *supra* note 89.

[103] *See* GDPR, art. 6(1)(f) ("Processing shall be lawful only if . . . processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.").

[104] *See* EDPB, *supra* note 89, at 5.

[105] *Id.* at 5-6.

[106] GDPR, art. 49.

[107] *Id.* art. 49(1)(d) (". . . the transfer is necessary for important reasons of public interest . . .").

[108] *See* EDPB, *supra* note 89, at 6.

[109] *See* GDPR, art. 49(1)(e) (". . . transfer is necessary for the establishment, exercise or defense of legal claims . . .").

[110] *See* EDPB, *supra* note 89, at 6.

However, "a close link is necessary between the data transfer and a specific procedure . . . and the derogation cannot be used to justify the [data] transfer . . . on the grounds of the mere possibility that legal proceedings may be brought in the future."[111] Likewise, possibility of data transfer under Article 49(1)(f) is also dismissed under the same reasoning mentioned above for Article 6(1)(d).[112] Lastly, the EDPB and the EDPS declared that the last paragraph of Article 49(1) "cannot provide a valid lawful ground to transfer personal data on the basis of [the] US CLOUD Act requests" mainly because, in addition to the balancing test imposed under Article 6(1)(f), the CSPs who are transferring the data must "notify both the supervisory authority and the data subject[, which] appears incompatible with 'protective orders' often joined to [the] US CLOUD Act warrants, which aim at maintaining the secrecy of the request (in order to avoid compromising the investigation)."[113]

2. Australia and the Assistance and Access Act

On December 9, 2018, the Australian government enacted a new legislation—the Assistance and Access Act (AAA)[114]—"to facilitate law enforcement access to data" and address problems associated with "cross-nature of investigations involving digital evidence."[115] The relevant provisions "specif[y] in detail the

[111] *Id*. at 6-7.

[112] *See* GDPR, art. 49(1)(f) ("In the absence of an adequacy decision [or of appropriate safeguards], a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions . . . (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.").

The EDPB and EDPS clarifies that the "circumstance that data subjects should be physically or legally incapable of giving consent . . . may not exclude situations where the data subject is constituting an imminent threat to the life and physical integrity of other persons, providing that sufficient information is provided to establish the validity of transfer in such circumstances." EDPB, *supra* note 89, at 7.

[113] *See* EDPB, *supra* note 89, at 7.

[114] *See Assistance and Access Act 2018* (Cth) ss 43A, 43B (Austl.), https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6195_aspassed/toc_pdf/18204b01.pdf;fileType=application%2Fpdf.

[115] Jennifer Daskal, *Privacy and Security Across Borders*, 128 YALE L.J. 1029,

requirements that apply if and when the government . . . accesses a computer or data known to be located across borders."[116]

The LCA identified three issues with the CLOUD Act, two of which seem to be more problematic and, thus, may prevent Australia from entering into an executive agreement with the United States under the CLOUD Act: (1) the lack of the enforcement of decryption on the CSPs, and (2) the requirement of review or oversight by the judicial or other independent authority.[117] More specifically, the CLOUD Act makes clear that the executive agreements cannot enforce an obligation on a CSP capable of decrypting data to do so.[118] But the AAA allows the Australian law enforcements to require the CSPs to decrypt private communications for criminal investigation purposes in certain situations.[119] In regards to the other incompatibility, the order issued by the QFG under the CLOUD Act must be "subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order."[120] However, the AAA "does not provide sufficient requirements for the independent judicial oversight" of the issuance of such orders.[121]

1031 (2018-2019).

[116] *Id*.

[117] *See* Law Council of Australia (LCA), Review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* 2018 (Cth), 8 (July 16, 2019), https://www.lawcouncil.asn.au/docs/e3857998-50d8-e911-9400-005056be13b5/3646%20-%20Review%20of%20the%20amendments%20made%20by%20the%20Assistance%20and%20Access%20Act.pdf.

[118] 18 U.S.C. § 2523(b)(3) ("[T]he terms of the [executive] agreement shall not create any obligation that providers be capable of decryption data or limitation that prevents providers from decrypting data.").

[119] *See* Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) (Austl.), https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6195_ems_1139bfde-17f3-4538-b2b2-5875f5881239/upload_pdf/685255.pdf;fileType=application%2Fpdf.

[120] 18 U.S.C. § 2523(b)(4)(D)(v).

[121] LCA, *supra* note 117, at 9. The Law Council of Australia notes that while the Technical Assistance Notices (TAN) and Technical Capability Notices (TCN)—which are equivalent of orders—require supervision of the Attorney General, the Attorney General is not an independent party as a member of the Executive Branch. For detailed discussions of TAN and TCN, *see* Law Council

Thus, the LCA, in its submission to the Australian Parliament, concluded that Australia, with its current legislation, will not qualify for an executive agreement with the United States under the CLOUD Act.[122] To be sure, these are incompatibilities under the current laws as they stand. That is to say, both parties will be able to agree on modified terms in an executive agreement. As of October 7, 2019, the United States and Australia have released a joint statement indicating that negotiations under the CLOUD Act are underway.[123]

D. U.S.-UK Executive Agreement of 2019

On the other hand, the United Kingdom has been a fervent supporter of the CLOUD Act, and it came with no surprise that it was the first country to have entered into an Executive Agreement under the statute.[124] In fact, the two countries had been negotiating a similar agreement even before the CLOUD Act was signed into law.[125] Section I.D.1 will briefly touch on the terms of the Executive Agreement that are relevant for the purposes of this Article.

---

of Australia, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Oct. 18, 2018), https://www.lawcouncil.asn.au/docs/508b2589-9ed2-e811-93fc-005056be13b5/3530%20-%20Telecommunications%20and%20Other%20Legislation%20Amendment%20Assistance%20and%20Access%20Bill%202018.pdf.

[122] *See* LCA, *supra* note 117, at 8.

[123] Press Release, U.S. Dep't of Just., Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton (Oct. 7, 2019), https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us.

[124] Drew Mitnick, *What Happened with the CLOUD Act (and What Comes Next)*, ACCESS NOW (Mar. 27, 2018), https://www.accessnow.org/what-happened-with-the-cloud-act-and-what-comes-next/ ("The first country that the U.S. will likely reach an agreement with is the United Kingdom . . .").

[125] *See* Ellen Nakashima & Andrea Peterson, *The British Wants to Come to America – with Wiretap Orders and Search Warrants*, THE WASH. POST (Feb. 4, 2016), https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html.

1. Relevant Sections of the Executive Agreement

DOJ emphasized that the Executive Agreement was recognized as necessary by both parties in order to fight "serious crimes."[126] The Executive Agreement is to be entered into force after a 180-day Congressional review period as required by the CLOUD Act.[127]

First, Article 1(16) limits the scope of the application of the Agreement to data that are used or controlled by a "Covered Person" but not by any "Receiving Party."[128] Article 1(12) clarifies that a "Receiving Party Person" is essentially a citizen, a permanent resident, or a government official of the United States[129] or that of the United Kingdom, or a corporation or any other person within the United Kingdom.[130] These two articles imply that the Executive Agreement, on its face, does not authorize the UK government to gather information involving U.S. citizens, either directly or indirectly.

When the UK or the U.S. government issues an order requesting relevant data from the CSPs within their jurisdictions, only their respective domestic laws apply.[131] This means that no laws of the United States will be relevant or applicable to the UK government's request for information from the U.S.-based CSPs within its borders.

Article 5 of the Agreement speaks to the requirement of "reasonable justification" in issuance of the orders and their judicial oversight by the UK courts.[132] Article 5(4) does not allow for orders that are issued for the purpose of disclosing information to the U.S. or a third-party government.[133] Articles 5(11), (12) elaborate on procedures through which the CSPs may object to such orders if they believe the order is inappropriate.[134] Essentially, a CSP may

---

[126] U.S. Dep't of Just., *supra* note 20 ("Attorney General William Barr said: "This agreement will enhance the ability of the United States and the United Kingdom to fight serious crime—including terrorism, transnational organized crime, and child exploitation . . . .").

[127] *See* 18 U.S.C. § 2523(d)(4). *But see infra* note 235.

[128] *See* U.S.-UK/Ir. Executive Agreement, *supra* note 28.

[129] *Id*. art. 1(16).

[130] *Id.* art. 1(12).

[131] *Id*. art. 3(2).

[132] *Id.* art. 5(1), (2).

[133] *Id.* art. 5(4).

[134] *Id*. art. 5(11), (12). *See also infra* notes 228-231 and accompanying texts.

object to the UK government's order, and if the two parties cannot resolve the issue, then the U.S. government will step in to evaluate the appropriateness of the order. If the U.S. government agrees with the objecting CSP, then the latter party will have no obligation to disclose any information to the UK government.

The most relevant part of the Agreement is Article 7: Targeting and Minimization Procedures, which takes a similar form of § 702 of FISA.[135] Article 7 requires the United Kingdom to "adopt and implement appropriate procedures to minimize" incidentally obtaining data of U.S. citizens while collecting data of a target person under its judicial order, i.e., incidental collection of such data. Article 7(3) requires the UK government to "segregate, seal, or delete, and not disseminate" such data that is not necessary to the criminal investigation and prosecution of the "Covered Person."[136]

Putting aside the difficulty of segregating data in general, the agreement does not elaborate on what constitutes "necessary," which is left for interpretation by the UK government. Article 7(5) requires that such data not be transmitted to the U.S. government unless it "relates to significant harm [or] threat to the United States."[137] Again, the Executive Agreement does not go far enough to define the extents of "relates" and "significant harm." However, the existence of Article 7(5) indicates that both parties recognize that the possibility of incidental collection of data is real and high, if not inevitable.

Lastly, according to the Executive Agreement, the United Kingdom does not require permission to use data obtained unless it raises freedom of speech concerns, and the United States needs to seek permission from the UK government only if the data obtained from a CSP server in the United Kingdom would be used for an offense that may result in the death penalty.[138]

---

[135] *See* 50 U.S.C. § 1801(h); *see also infra* notes 144-147 and accompanying text.

[136] *See* U.S.-UK/Ir. Executive Agreement, *supra* note 28, art. 7(3).

[137] *Id*. art. 7(5).

[138] *Id.* art. 8(4).

II. POTENTIAL JEOPARDY TO THE DATA PRIVACY OF U.S. CITIZENS

Having been enacted as part of an omnibus spending bill with haste,[139] the CLOUD Act includes gaps, some of which have been identified by foreign entities in Section I.C. Given the transnational nature of cross-border data transfers, the statute should have included details that would fill in such cracks. While the Executive Agreement does include terms that attempt to make whole the deficiencies, it does not provide adequate protection against incidental data collection. Part II argues that the possibility of incidental collection of data belonging to U.S. citizens is at least probable, if not certain. Section II.A, using FISA as a vehicle, identifies ways in which this could happen under the Executive Agreement. Section II.B discusses how this could happen under the UK laws that are arguably less than adequate to protect data privacy of individuals.

A. Incidental Collection of Data of Non-target Citizens

Incidental collection of data refers to the collection of data belonging to those who are not the target of criminal investigations.[140] For example, if the government is seeking private data of Citizen A—the target—and such data includes conversations between A and B, then data of B may be "incidentally" collected during the evidence gathering. Then, the data belonging to B would be entered into the database of the governmental organizations who are free to search within the database as long as any data sought is related to the investigation.[141]

Such incidental collection is nothing new. In fact, the government's recognition of its possibility is reflected in many regulations, including FISA and the CLOUD Act as well as the Executive Agreement.[142] More specifically, this is shown in §§ 2523(b)(2), (b)(4)(D)(vi)(G) and (H), as amended by the CLOUD Act, and Article 7 of the Executive Agreement which is written

[139] *See* Davis & Gressel, *supra* note 8.
[140] *See generally* BRENNAN CTR. FOR JUST., *supra* note 27.
[141] *Id*.
[142] *See infra* note 143.

almost in verbatim.[143] In Section II.A.1, FISA will be discussed because it illustrates the authorities given to governmental agencies that lead to incidental collections. The statute also includes provisions and structures that parallel those of the CLOUD Act and the Executive Agreement. Section II.A.2 provides a brief overview of the history of the UK surveillance laws that led to the current Investigatory Powers Act, which serves as the legal basis for the Executive Agreement for the European country.

1. The Foreign Intelligence Surveillance Act

As amended in 2008, § 702 of FISA authorizes the U.S. government to collect electronic communications of foreigners located outside of the United States from the CSPs if the data is related to national security or other serious crimes.[144] However, FISA mandates that data acquisition under § 702 must be consistent with the Fourth Amendment, and forbids the U.S. government from

[143] § 2523(b)(2) requires that a qualifying foreign government to have "adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement."

Additionally, § 2523(b)(4)(D)(vi)(G) requires the foreign government, "using procedures that, to the maximum extent possible, meet the definition of minimization procedures in Section 101 of [FISA], segregate, seal, or delete, and no disseminate material found not to be information that is, or is necessary to understand or assess the importance of information that is, relevant to the prevention, detection, investigation, or prosecution of serious crime, including terrorism, or necessary to protect against a threat of death or serious bodily injury harm to any person."

Finally, § 2523(b)(4)(D)(vi)(H) states that the qualifying foreign government "may not disseminate the content of a communication of a United States person to United States authorities unless the communication may be disseminated pursuant to subparagraph (G) and relates to significant harm, or the threat thereof, to the United States or United States persons including crimes involving national security such as terrorism significant violent crime, child exploitation transnational organized crime, or significant financial fraud."

Indeed, the U.S.-UK/Ir. Executive Agreement includes similar languages. *See* U.S.-UK/Ir. Executive Agreement, *supra* note 28; *see also infra* notes 144-147 and accompanying texts.

[144] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 § 702, 50 U.S.C. § 1881 (2008) [hereinafter FISA].

intentionally targeting data that belongs to U.S. citizens.[145] FISA also includes a provision on "minimization procedures" which is aimed to curtail the acquisition, retention, and dissemination of data of U.S. citizens that are collected unintentionally—or incidentally.[146] If collected, data of U.S. citizens may not be used in criminal proceedings unless certain exceptions apply.[147]

Many FISA provisions are similar to those in the CLOUD Act as well as the Executive Agreement. Some distinctions are just as apparent, however. For one, under FISA, initial certification submitted by the Attorney General for collection of data under § 702 is subject to review by the Foreign Intelligence Surveillance Court (FISC) to ensure that the certification is consistent with the Fourth Amendment.[148] On the other hand, the CLOUD Act and the Executive Agreement only require that the judicial order of the UK courts reflect "reasonable justification" based on the facts presented to them.[149]

Incidental collection can happen in two ways under § 702: downstream collection and upstream collection. Downstream collection, also known as the PRISM program, is when government agencies collect data from the CSPs if "communications contain certain terms chosen by the [National Security Agency]."[150] Upstream collection refers to massive data gathering by the National Security Agency directly from the internet which are transmitted through "domestic and international fiber optic cables."[151] This method allows for bulk data collection by the agency which may contain communications data of those other than the targeted

[145] *See id.* § 1881a(b).

[146] *See id.* § 1801(h).

[147] The use of incidentally collected data of U.S. citizens in criminal proceedings, while is an important issue, is beyond the scope of this paper, which is merely exploring the problems of similar collection in order to parallel the problem in the circumstances of the UK. For statutory language on how such data may be used in criminal proceedings, *see id.* § 1806.

[148] *See* 50 U.S.C. §§ 1805(a)(2)(A), (b).

[149] *See supra,* note 132.

[150] Ioanna Tourkochoriti, *The Transatlantic Flow of Data and the National Security Exception in the European Data Privacy Regulation: In Search for Legal Protection Against Surveillance*, 36 U. PA. J. INT'L L., 459, 462-463 (2014).

[151] *Id*. at 463.

persons.[152] Collected data is entered into a database routinely searched by government entities.[153] The agencies do not need a warrant to search the existing database, a practice is coined as "backdoor searches"[154] since they would need to show probable cause otherwise.[155]

Incidental collection of bulk data belonging to U.S. citizens under FISA is an ongoing problem. On October 18, 2019, the FISC released an opinion on the Federal Bureau of Investigations (FBI)'s use of its authority under § 702.[156] The opinion shows that such incidental collection is not-so incidental. In sum, the court found that the "querying procedures and minimization procedures [of the FBI] do not comply with the requirement at Section 702(f)(1)(B) [and] to be inconsistent with statutory minimization requirements and the requirements of the Fourth Amendment," particularly in relation to the use of backdoor searches.[157] Thus, even with the safeguards of annual judicial review and attempts to enforce the probable cause standard, the data of U.S. citizens has not been adequately protected by, but rather been exposed to, the U.S. government. Nonetheless, the FISC approved the data collection certification of the FBI in question, after the latter submitted amended certifications to explain why they are acquiring certain data.[158]

---

[152] Sneha Indrajit et al., *FISA's Section 702 & the Privacy Conundrum: Surveillance in the U.S. and Globally*, THE HENRY M. JACKSON SCH. OF INT'L STUD. (Oct. 25, 2017), https://jsis.washington.edu/news/controversy-comparisons-data-collection-fisas-section-702/.

[153] *Backdoor Search*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/backdoor-search.

[154] *Id*.

[155] Brittany Adams, *Striking a Balance: Privacy and National Security in Section 702 U.S Person Queries*, 94 WASH. L. REV. 401, 404 (2019).

[156] Foreign Intelligence Surveillance Court, *Documents Regarding the Section 702 2018 Certification* (Oct. 18, 2018), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf.

[157] *Id*.

[158] Aaron Mackey & Andrew Crocker, *Secret Court Rules that the FBI's "Backdoor Searches" of Americans Violated the Fourth Amendment*, ELECTRONIC FRONTIER FOUND. (Oct. 11, 2019), https://www.eff.org/deeplinks/2019/10/secret-court-rules-fbis-backdoor-searches-americans-violated-fourth-amendment.

Seeing as how even the Fourth Amendment does not seem to provide enough protection to data privacy, it is easy to imagine a situation where with a lesser stringent standard, violation of privacy rights may happen in a more consistent basis. This has been the key controversy surrounding the surveillance laws of the United Kingdom.

2. UK Public Surveillance Laws

The UK government has had its public surveillance laws challenged on numerous occasions. The UK surveillance regime has its roots in § 94 of the Telecommunications Act of 1984, which gave the government the authority to force communications providers to retain and provide relevant data.[159] This power had been used for decades by the government to collect data in bulk without any independent oversight.[160] A similar tool used by the UK government is the Regulation of Investigatory Powers Act of 2000 (RIPA), which authorized the government to collect certain types of private communication data without judicial oversight.[161] The product of the government's effort to supplement RIPA was the Data Retention and Investigatory Powers Act of 2014 (DRIPA). [162] DRIPA authorized the UK Secretary of State to compel communications providers to retain data for any purpose in relation to §22(2) of

[159] Telecommunications Act 1984, §§ 94(1), (2), (Eng.).

[160] Alan Travis et al., *Theresa May Unveils UK Surveillance Measures in Wake of Snowden Claims*, THE GUARDIAN (Nov. 4, 2015), https://www.theguardian.com/world/2015/nov/04/theresa-may-surveillance-measures-edward-snowden.

[161] Rubin S. Waranch, *Digital Rights Ireland Deja Vu?: Why the Bulk Acquisition Warrant Provisions of the Investigatory Powers Act 2016 Are Incompatible with the Charter of Fundamental Rights of the European Union*, 50 GEO. WASH. INT'L L. REV. 209, 215 (2017); *see also* Regulation of Investigatory Powers Act 2000, c. 23 (Eng.), http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf.

[162] *See State Surveillance and Data Privacy: What Now?*, EACHOTHER (Sept. 21, 2018), https://eachother.org.uk/state-surveillance-what-now/ (explaining that DRIPA was passed after failed attempt by Home Secretary Theresa May to introduce the Communications Data Bill that would "grant[] even wider surveillance powers" than RIPA, a seemingly outdated law in light of recent digital advancements).

RIPA.[163] After its expiration, DRIPA was struck down by the UK Court of Appeals, following the Court of Justice of the European Union (CJEU)'s judgement against it because of its inconsistencies with the data retention laws of the EU and for the lack of independent oversight.[164] For similar reasons, the Investigatory Powers Tribunal[165] ruled that data collection implemented by the government under DRIPA was not compatible with Article 8 of the European Convention on Human Rights, which includes provisions of individual's fundamental right to protection of privacy.[166]

The most recent statute that grants the UK government similar, and arguably more expansive, authority to seek citizens' data for national security purposes is the Investigatory Powers Act (IPA), passed in 2016.[167] At the time of enactment, the IPA authorized governmental agencies to collect bulk of communications data, rather than only those of targeted individuals, upon approval by the Secretary of State.[168] The IPA went through some amending in 2018, during which the government conceded that DRIPA was inconsistent with the EU law because not all of the data retained was for the purpose of fighting "serious crime," their collection was not subject to review by independent body, and the IPA originally had provisions taken from DRIPA.[169] As amended, the IPA includes

[163] *See* Data Retention and Investigatory Powers Act 2014, c. 27, § 1(1), (Eng.).

[164] Matt Burgess, *The UK's Mass Surveillance Laws Just Suffered Another Hefty Blow*, WIRED (Jan. 30, 2018), https://www.wired.co.uk/article/uk-surveillance-unlawful-watson-davis.

[165] The Investigatory Powers Tribunal, established in 2000 as an independent judicial tribunal under RIPA, is the equivalent of the FISC in the United States. *See General Overview and Background,* THE INVESTIGATORY POWERS TRIB. (July 5, 2016), https://www.ipt-uk.com/content.asp?id=10. However, the Tribunal will not be discussed at length because, as of this writing, much of its role has been transferred to the Investigatory Powers Commissioner's Office created by the more recent Investigatory Powers Act. *See Who We Are*, INVESTIGATORY POWERS COMM'R'S OFF., https://www.ipco.org.uk/.

[166] Privacy Int'l v. Secretary of State for Foreign and Commonwealth Affairs [2016] IPT 15, 110-CH (Eng.), https://www.ipt-uk.com/docs/Bulk_Data_Judgment.pdf; *see also* Matt Burgess, *MI6, MI5 and GCHQ 'Unlawfully Collected Private Data for 10 Years'*, WIRED (Oct. 17, 2016), https://www.wired.co.uk/article/uk-collect-data-unlawful.

[167] *See* IPA, *supra* note 23.

[168] *See* Waranch, *supra* note 161, at 227.

[169] Ian Cobain, *UK Has Six Months to Rewrite Snooper's Charter, High Court*

definitions of "serious crimes"[170] and created the Investigatory Powers Commission (IPC)—a group of judges who provide independent oversight of the process.[171] As of this writing, several challenges to the IPA have not been successful in the UK Courts.[172]

B. Incidental Collection under the Executive Agreement

As mentioned above, governments themselves recognize that incidental collection of non-target citizens is probable, if not inevitable. FISA elaborates on minimization procedures to ensure that incidentally collected data of U.S. citizens are not abused.[173] Likewise, the Executive Agreement includes provisions that the UK government must abide by if data of U.S. citizens are incidentally collected. More specifically, in regards to such data, the UK government must evaluate whether the data is imperative to the investigation and must destroy the data if not, and cannot hand over such data to the U.S. government unless it is related to national security of the United States.[174] However, the IPA may create ways in which the UK government not only collect but retain data that belongs to U.S. citizens. This Section identifies two issues: the limited oversight of bulk collection of data and the lack of probable cause standard in the United Kingdom.

Rules, THE GUARDIAN (Apr. 27, 2018), https://www.theguardian.com/technology/2018/apr/27/snoopers-charter-investigatory-powers-act-rewrite-high-court-rules.

[170] The IPA defines "serious crime" as "offence, or one of the offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 18 . . . and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more [or where] the conduct involves use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose." *See* IPA, *supra* note 23, § 263(1).

[171] *Id.* c. 25.

[172] *See* Carey, *supra* note 25.

[173] *See* 50 U.S.C. § 1801(h).

[174] *See* U.S.-UK/Ir. Executive Agreement, *supra* note 28, art. 7(5).

1. Bulk Data Collection

Traditionally, one common issue that has constantly been at the center of controversy over the UK surveillance laws is the purpose of data collections. In the past, certain local authorities had used powers granted under RIPA for reasons that are not related to national security or terrorism—to monitor dog barking, gather evidence against those guilty of feeding pigeons, or checking up on government benefit claimants, for example—as the statute itself defines as its purpose.[175] While these instances happened before the enactment of the IPA, which supposedly has more stringent requirement and oversight, they illustrate how the surveillance laws can be abused without the knowledge of the public.

In *Digital Rights Ireland and Seitlinger & Others*, the CJEU struck down the Data Retention Directive of the European Union[176] because the retention of data of citizens violated fundamental rights to privacy illustrated in Articles 7 and 8 of the Charter of Fundamental Rights.[177] In its opinion, however, the CJEU did acknowledge that preventing and prosecuting "serious crimes" is an acceptable justification for collection and retention of data by government authorities.[178] In response to this judgement, the United Kingdom passed DRIPA to provide a legal basis to continuously force the CSPs to retain communications data of the citizens. Upon its expiration, DRIPA was replaced by the IPA.[179]

Under the IPA, in order for law enforcement agencies to obtain a warrant for bulk acquisition, the UK Secretary of State must

[175] Anushka Asthana, *Revealed: British Councils Used RIPA to Secretly Spy on Public*, THE GUARDIAN (Dec. 25, 2016), http://www.theguardian.com/world/2016/dec/25/british-councils-used-investigatory-powers-ripa-to-secretly-spy-on-public.

[176] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105).

[177] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger & Others, 2014 E.C.R. 238.

[178] *Id.* ¶ 102.

[179] David Fennelly, *Data Retention: the Life, Death and Afterlife of a Directive*, J. ACAD. OF EUR. L. 673, 685 (2019), https://doi.org/10.1007/s12027-018-0516-5.

approve the warrant with a belief that the warrant is (1) in the interest of national security, (2) for the purpose of preventing or detecting serious crime, or (3) in the interest of economic well-being of the United Kingdom as long as it relates to the interests of national security.[180] The Secretary also needs to consider whether the collection authorized by the warrant is proportionate to the purpose it is sought to achieve.[181] Then, the judicial commission must approve the warrant. In doing so, the commission is to determine whether the warrant satisfies *any* of the three purposes mentioned above as well as whether the scope of the warrant is proportionate to what is sought to achieve.[182]

However, the IPA itself does not indicate which factors must be taken into account in making such decisions, and, thus, provides ample room for discretion of the Secretary.[183] For example, it does not clarify what constitutes as "interest of national security" or "economic well-being."[184] This allows for much leeway in validating an issuance of a warrant and broad inclusion of data to be collected.[185] In addition, the purposes identified by agencies in order to obtain a warrant is, by its inherent nature, confidential.[186] As a result, it will be difficult to examine what exactly were the reasons cited in their requests for warrants permitting bulk data collection.

To be sure, the language of "national interest" and "serious crime" is almost identical to the limitations set by the Executive Agreement.[187] But, assuming that bulk collection of data inevitably exposes communications data that belong to U.S. citizens, the UK government's request for disclosure from U.S.-based CSPs may

[180] *See* IPA, *supra* note 23, c. 25, §§ 158(1), (2).

[181] *Id*. A comprehensive list of valid operational purposes shared by the government shows broad spectrum of purposes that may potentially qualify for issuance of such warrant. *See* Operational Case for Bulk Powers, GCHQ, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf.

[182] *See* IPA, *supra* note 23, c. 25, §§ 23, 140, 159.

[183] *See* Waranch, *supra* note 161, at 227.

[184] *Id.* at 231.

[185] *Id.* at 233.

[186] *Id*. at 234.

[187] *See supra* note 82.

violate the data privacy of U.S. citizens since the disclosure is governed by the UK laws, only.[188]

2. Judicial Standard of Reasonable Justification

In the United States, the Fourth Amendment is the primary safeguard against the government's investigatory power.[189] In the context of electronic evidence, the U.S. government needs to obtain a judicial warrant in order to collect relevant data from the CSPs. The government has the burden of proving "probable cause" in front of the FISC to obtain approval.[190]

For the United Kingdom, the most equivalent legal safeguard against intrusion of privacy is Article 8 of the European Convention on Human Rights, which states that privacy is a fundamental human right.[191] Article 8 is also the basis on which the CJEU ruled against parts of the UK's surveillance regime in *Big Brother Watch and Others v. United Kingdom*.[192] While the Court in *Big Brother Watch* did not assess the IPA directly, it found that bulk interception of communications and obtainment of data from the CSPs by the UK government violated the Article.[193] One of the reasons cited was the insufficient oversight of such collection by the UK Investigatory Powers Tribunal.[194]

The CLOUD Act and the Executive Agreement only require that the UK courts find "reasonable justification" that the disclosure of data from the CSPs is warranted.[195] Because both documents recognize that only the UK laws will govern the procedure in the

[188] *See* U.S.-UK/Ir. Executive Agreement, *supra* note 28, art. 3(2).

[189] *See* Gonzalez, *supra* note 10, at 23.

[190] *See supra* note 148.

[191] European Court of Human Rights on Guide on Article 8 of the European Convention on Human Rights (Aug. 31, 2019), https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

[192] Big Brother Watch and Others v. the United Kingdom, 299 Eur. Ct. H.R. __ (2018), https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-6187848-8026299%22]}.

[193] *Id*. at 3-4.

[194] Sean Gallagher, *"Bulk Interception" by GCHQ (and NSA) Violated Human Rights Charter, European Court Rules*, ARS TECHNICA (Sept. 13, 2018), https://arstechnica.com/tech-policy/2018/09/bulk-interception-by-gchq-and-nsa-violated-human-rights-charter-european-court-rules/.

[195] U.S.-UK/Ir. Executive Agreement, *supra* note 28, art. 5(1), (2).

United Kingdom, probable cause standard required by the Fourth Amendment will play no role in the issuance of judicial order by the UK authorities. As mentioned above, the IPC needs to consider whether the warrant signed by the Secretary of State is related to acceptable and legitimate objectives and the collection of data is proportionate to achieving that goal.[196] In doing so, the IPC will most likely adopt the reasonable justification standard set by UK courts,[197] which has a lower burden of proof than the probable cause standard.[198] This lack of protection under the Fourth Amendment will increase the possibility of incidental collection of U.S. citizens' data in the process of collecting that of targeted UK citizens by the UK government.

III. ADOPTING EU STANDARDS AND INCREASING CSPS' ROLES

While it is clear that incidental collection of data is a problem that the lawmakers were aware of, neither the CLOUD Act nor the Executive Agreement indicates any specific solution to *prevent* the collection of such data in the first place. On the other hand, recognizing privacy as one of the fundamental rights, the EU has been at the forefront of developing strong data protection laws globally.[199] This Part looks at the legal regime implemented by the EU to ensure the protection of consumer data, and how a similar approach could fill in the gap.

To this end, Section III.A highlights transferrable aspects of approaches taken by the European bloc. It should be noted that while adopting some of the approaches taken by the bloc would make the data transfer between the United States and the United Kingdom safer in theory, this will be easier said than done due to differences in laws and policies of the EU and the United States. For instance, the EU recognizes its citizens' Right to be Forgotten while it lacks

---

[196] *See* IPA, *supra* note 23, c. 25, §§ 23, 140, 159.

[197] *Id.*, c. 25, § 23(2)(a) ("In deciding whether to approve a [warrant under the IPA,] the Judicial Commissioner must—(a) apply the same principles as would be applied by a court on an application for judicial review. . .").

[198] *See* Gonzalez, *supra* note 10 (arguing that the tests used by the Investigatory Powers Commission in its proportionality assessment of warrant for decryption under the Investigatory Powers Act is a low bar).

[199] *See* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 131-170 (2020).

the Fourth Amendment rights protected by the U.S. Constitution. Another difference between the two is each entity's treatment of data privacy: in the United States, it is treated as a transferrable commodity whereas the EU considers data privacy to be a fundamental human right.[200]

Thus, Section III.B discusses alternative, and perhaps complementary, methods to achieve the same goal: the increased role of the private sector, namely the CSPs. That Section will focus on how they may also contribute to the protection of data privacy of U.S. Citizens when data transfers are executed under the CLOUD Act and the Executive Agreement. This may require some modification of the two, which also will not come easily. However, as seen from the CSPs support of the CLOUD Act in the first place, it seems that they would be willing to take more of an active role, making it a possible solution.[201]

A. Legislative Amendments in Reference to the GDPR

Few would question the relatively dominating role of the EU in shaping the data privacy laws around the globe. It is said that this effect is likely to continue for some time despite the steady decreases in the EU's market share in the digital economy with the rise of other countries such as China and India.[202] Section III.A.1 looks at how the CLOUD Act may be amended to include increased oversight in the process of evaluating candidate countries and determining whether they qualify for executive agreements. In doing so, that Section discusses the procedures taken by the EU in evaluating candidacy for Adequacy Decisions under the GDPR.[203] Also

[200] *See id*.

[201] *See Support for the CLOUD Act of 2018*, MICROSOFT (Apr. 11, 2018) https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/04/Support-for-the-CLOUD-Act-of-2018_4.11.18.pdf.

[202] *See* BRADFORD, *supra* note 199.

[203] To be sure, the CLOUD Act deals with cross-border data transfers for the purpose of criminal investigation, while the Adequacy Decisions—which deals with personal data transfer for commercial purposes—do not. However, because this Section looks at the procedures taken before the Adequacy Decision is granted to another country, this difference has no significance. Emphasis is given to the symmetry of the purposes behind Adequacy Decisions and the CLOUD Act to ease transfer of private data without additional procedure and authorization.

looking at the corresponding Articles in the GDPR, Section III.A.2 proposes legislative amendments to the CLOUD Act which may provide rights to remedy and to file a complaint under the statute to private persons.

1. Amending the Process of Evaluating QFGs

Article 45 of the GDPR addresses the Adequacy Decisions, a method allowed under the Regulation through which private entities can transfer personal information of data subjects to other countries or international organizations.[204] Foreign countries seek Adequacy Decisions from the EU which, if granted, allow businesses operating in both countries to transfer commercial data beyond their borders with ease. Before granting an affirmative decision, the bloc goes through a rigorous process of evaluating the adequacy of privacy protection laws in candidate countries.[205]

For example, the European Commission issued an Adequacy Decision with Japan in January 2019.[206] The final adoption came only after the Japanese government's adoption of Supplementary Rules which enhanced the country's existing privacy laws to provide as robust data protection as the GDPR.[207] As of this writing, the EU has a similar ongoing negotiation with the Republic of Korea (Korea). Korea sought Adequacy Decisions with the EU in 2015, but the European Commission flagged the inadequate independence of the relevant enforcement bodies.[208] More specifically, under the

[204] *See* GDPR, art. 45.

[205] EUR. COMM'N., *Digital Single Market – Communications on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers* (Jan. 10, 2017) ("An adequacy decision is a decision taken by the Commission establishing that a third country provides a comparable level of protection of personal data to that in the European Union, through its domestic law or its international commitments. As a result, personal data can flow from the [EU] to that third country, without being subject to any further safeguards or authorisations.").

[206] Věra Jourová, EUR. COMM'N., *EU Japan Adequacy Decision* (Jan. 2019). https://ec.europa.eu/info/sites/info/files/research_and_innovation/law_and_regulations/documents/adequacy-japan-factsheet_en_2019_1.pdf.

[207] *See id*.; *see also* EUR. COMM'N., *International Data Flows: Commission Launches the Adoption of its Adequacy Decision on Japan* (Sept. 5, 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5433.

[208] David Meyer, *South Korea's EU Adequacy Decision Rests on New*

Korean data protection law, the Personal Information Protection Act, the enforcement power lied with the Ministry of Interior and Safety.[209] The most recent amendment passed in the peninsular country on January 9, 2020, was specifically aimed at successfully obtaining an Adequacy Decision from the EU by creating an independent agency.[210]

The EU has adopted adequacy decisions for the following countries and territories: Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and Japan.[211] Currently, there is a partial Adequacy Decision granted by the EU for the United States, meaning only *some* data may be transferred between the two countries under limited circumstances.[212] In assessing the adequacy of the data protection laws of a country, the European Commission looks at similar elements that the U.S. Attorney General is to consider under the CLOUD Act in evaluating foreign governments as candidates for an executive agreement. Some similar elements are, among others, laws protecting human rights and privacy, and clear procedures to achieve this objective.[213]

However, one clear distinction is that the process of evaluating a foreign country's privacy laws and ultimately adopting Adequacy

Legislative Proposal, IAPP (Nov. 27, 2018), https://iapp.org/news/a/south-koreas-eu-adequacy-decision-rests-on-new-legislative-proposals/.

[209] Articles 52 and 53 of the GDPR requires an independent supervisory authority within the country that seeks Adequacy Decision from the EU. *Id.*

[210] Personal Information Protection Commission, *2019 Annual Report: Personal Information Protection in Korea*, 131-32 (Aug. 30, 2019), http://www.pipc.go.kr/ebook/y201908/index.html (S. Korea).

[211] *Adequacy Decisions: How the EU Determines if a Non-EU Country has an Adequate Level of Data Protection*, EUR. COMM'N., https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[212] This limitation is due to the EU's stance that there are some parts of the data privacy law in the United States that are inadequate. *See* EUR. COMM'N., *supra* note 205("The EU-U.S. Privacy Shield framework is a 'partial' adequacy decision, as , in the absence of general data protection law in the U.S., only the companies committing to abiding by the binding Privacy Shield principles benefit from easier data transfers.").

[213] For non-exhaustive elements that must be considered by the European Commission in assessing the adequacy of the level of data protection of a prospective country, *see* GDPR, art. 45(2)(a).

Decisions involves relatively more inputs from other independent authorities. The process involves (1) a proposal from the European Commission with (2) reference to an opinion of the EDPB which consists of one representative from each Member State pursuant to Article 68 of the GDPR, (3) approval by representatives of the Member States, and, finally, (4) the adoption decision by the European Commission.[214] By contrast, the CLOUD Act explicitly states that the Attorney General's final determination will not be subject to any judicial or administrative review.[215] To be sure, under the CLOUD Act, the Attorney General's evaluation of a QFG and the final executive agreement is subject to review by Congress.[216] But the statute, which does *not* require affirmative approval of the Legislative branch but rather only mandates that Congress object if unsatisfied, fails to elaborate what would happen if Congress does not review the executive agreements.[217] In that scenario, the Executive Branch would be the *de facto* sole determiner of qualifying governments.

The authority to evaluate a foreign government could also be given to an independent authority in addition to the Attorney General. At minimum, an independent agency or a committee should have the authority to approve or disapprove the decision of the Attorney General. This would decrease the possibility of the United States entering into an executive agreement with a foreign government whose data protection laws are inadequate to minimize the incidental collection or abuse of data of U.S. citizens, and, thus, breach of their privacy.

2. Cause of Action and Remedy for Private Persons

As it stands currently, the Executive Agreement does not give rise to any right or remedy on the part of private persons.[218]

---

[214] *See* EUR. COMM'N., *supra* note 211.

[215] *See* 18 U.S.C. § 2523(c) ("Limitation on Judicial Review—A determination or certification made by the Attorney General under subjection (b) shall not be subject to judicial or administrative review.").

[216] *See* 18 U.S.C. § 2523(d)(4).

[217] *See id.*

[218] *See* U.S.-UK/Ir. Executive Agreement, *supra* note 28, art. 3(4) ("The provisions of this Agreement shall not give rise to a right or remedy on the part of any private person, including to obtain, suppress or exclude any evidence, or to

Incorporation of provisions similar to Chapter VIII of the GDPR would invoke additional efforts by the CSPs and the QFG to ensure that collection of U.S. citizens' data does not occur. Simply put, Chapter VIII of the GDPR grants data subjects the right to file a complaint under the Regulation to seek judicial remedies against the government entities and the CSPs in cases of data breach.[219] If the data subjects suffered damages, the CSPs will also have to compensate the victims,[220] and any other infringement may subject the CSPs to administrative fines[221] as well as penalties under the laws of the Member States.[222]

The CLOUD Act and the Executive Agreement should be modified to carve out instances that give cause of action to U.S. citizens when their data has been incidentally collected. Of course, to be compatible with the Executive Agreement, the right should not be exercised to obstruct criminal investigations. Further amendment should provide for remedies *ex post* so that the requesting QFG and the CSPs would be more cautious in identifying the data that belongs to U.S. citizens.

Similarly, the Executive Agreement and the CLOUD Act could be further amended to impose obligations on the CSPs to take sufficient efforts to ensure that U.S. citizens' data is not sent to the QFGs, and, if any material data belong to U.S. citizens are identified, to take adequate steps to quash or modify the motion pursuant to the Agreement. Enforcing fines and penalties to inadequate measures taken by CSPs when they reasonably knew or should have known the inclusion of U.S. citizens data in their transfers may also provide additional safeguards.

B. Increasing the Role of the CSPs

Another solution is to have the CSPs take more active roles in data collection under the CLOUD Act and executive agreements. Neither the CLOUD Act nor the Executive Agreement requires the

impede the execution of Legal Process.").

[219] *See* GDPR, art. 77, 78, 79.

[220] *Id.* art. 82.

[221] *Id.* art. 83.

[222] *Id.* art. 84.

CSPs to comply with requests of data by the UK authorities.[223] At the same time, they do not require the CSPs to take any additional measures to safeguard the data of U.S. citizens. Adopting some of the specific requirements the CSPs must abide by under the GDPR into the executive agreements or the CLOUD Act may provide additional protection of U.S. citizens' privacy. Section III.B.1 proposes requiring the CSPs to provide notifications to the consumers in instances of privacy breach via incidental collection. Section III.B.2 proposes implementing procedures under which the CSPs could file Motions to Quash and/or Modify judicial orders granted by foreign courts with less stringent standard if potentiality of incidental collection is identified.

1. Notification Obligation

Article 7 of the GDPR requires the CSPs to obtain explicit consent from the users in terms of how their data is processed.[224] At least with respect to U.S. citizens who are identified to be using services from the U.S.-based CSPs, the providers should be required to explicitly disclose that their data is not to be collected by the foreign authorities. While doing so, the CSPs could ask for consent were this to be the case for the purposes identified in the underlying executive agreements. This would be the simplest and the easiest way to solve the problem of incidental collection, for the collection would have been agreed upon by the U.S. citizens *ex ante*. However, it is unlikely that many U.S. persons would agree to have their private information exposed. Taking this step, nonetheless, would at least inform the users of the possibility of incidental collection of their data and increase awareness of the problem.

Currently, the CLOUD Act does not create any obligation on the CSPs to take such action, but they are subject to the domestic law of the QFG.[225] This means, for example, the CSPs have no obligation to notify the U.S. citizens' whose data has been collected by the UK government unless the UK law requires such notification. An

[223] *See* 18 U.S.C. § 2523(b)(4)(D)(iii); *see also* U.S.-UK/Ir. Executive Agreement, *supra* note 28, art. 6(3).

[224] *See* GDPR, art. 7.

[225] *The Purpose and Impact of the CLOUD Act – FAQs*, U.S. DEP'T OF JUST., https://www.justice.gov/dag/page/file/1153466/download.

obligation can be imposed upon the CSPs to notify the U.S. citizens when their data has been transferred to a QFG. If enforced, such requirements would parallel Article 19 and Article 34 of the GDPR. Article 19 requires the CSPs, upon request by the data subjects, to inform the consumers of the recipients of their data.[226] By contrast, under Article 34, the CSPs have affirmative obligation to notify to the data subjects if their data has been breached.[227] Combining these rules, the CSPs can be required to provide detailed notification when consumer data has been transferred to a QFG under the executive agreement. While this obligation by itself may not prevent all incidental collections, in conjunction with other remedies mentioned above, it will increase the role of the CSPs in making sure the data requested by, and transferred to, QFGs do not include personal information of U.S. citizens.

2. Objection to Search Warrants

The CLOUD Act allows the CSPs to file a motion to quash or modify a search warrant if they reasonably believe that disclosure of requested data would violate the laws of a QFG.[228] However, the language of the statute suggests that this only applies to CSPs move to modify or quash judicial orders in the United States.[229] The only other provision that seems to apply to Motions to Modify or Quash judicial orders in a foreign court is 18 U.S.C. § 2703(d), which allows the court to grant such motion "if the information or records requested are unusually voluminous" or "compliance with such

[226] *See* GDPR, art. 19.

[227] *Id.* art. 34.

[228] *See* 18 U.S.C. § 2703(h)(2)(A)(ii); *see also supra* notes 77-80 and accompanying texts.

[229] The relevant provisions do not specify whether they are referring to courts in the United States or in the QFGs. *See generally id*. § 2703(h)(2). But the CSPs must show that the consumer is not a U.S. person, and, thus, the request is inappropriate—which would be the case only if the judicial order was obtained by the United States to obtain data of a non-U.S. person. Moreover, the provisions on comity analysis directs the court with such motion to take into consideration "the interest of the United States," *id.* § 2703(h)(3)(A), and "the interests of the [QFG] in preventing any prohibited disclosure." *Id.* § 2703(h)(3)(B). Therefore, the only provision in the CLOUD Act that speaks to Motions to Modify or Quash search warrant seems to apply in U.S. courts only.

order otherwise would cause an undue burden on [the CSPs]."[230] The Executive Agreement merely states that the CSPs may make objections to the UK government "when it has reasonable belief that the Agreement may not be properly invoked with regards to the [search warrant]" upon issuance of the order for disclosure.[231] No other relevant detail is present in the document.

In theory, a U.S.-based CSP should be able to object to the search warrants issued by the UK authorities given that it believes that the order does not meet the requirements set by the CLOUD Act and the Executive Agreement. However, the likelihood of success is questionable, especially given the lack of specificity as to how foreign courts should deal with such objections. As discussed, persons in the United Kingdom do not enjoy the equivalent protection of the Fourth Amendment. Rather, satisfaction of a reasonable justification standard by the UK authorities is sufficient to issue an order. And because only the UK laws apply according to the Executive Agreement,[232] the CSPs will not be able to object to the issued order even if they believe that there is no probable cause for the order. To be clear, this would not be a problem if only the data of UK citizens are requested. But when there are possibilities that data belonging to U.S. citizens may also be collected, and even if the CSPs are aware of such possibilities, there is no ground for objection under the current statute and the Executive Agreement since both documents only refer to *intentionally targeted persons* who are, presumably, the UK citizens.[233]

It is less realistic to force the probable cause standard onto all the warrants issued by the UK authorities. But it may be possible to enforce such standard when data belonging to U.S. persons is involved. One solution is to allow for review by the U.S. authorities early on in the process if the CSPs can show that the disclosure of data of the targeted UK person would also include that of U.S. persons. A creation of a separate procedure may allow an independent authority within the U.S. government to review the order, for example. But there is an uneasy possibility that this additional step might defeat the original purpose of the CLOUD Act

---

[230] *Id.* § 2703(d).
[231] U.S.-UK/Ir. Executive Agreement, *supra* note 28, art. 5(11).
[232] *See id.* art. 3(2).
[233] *See id.* art. 4(3); *see also* 18 U.S.C. § 2523 (b)(4)(A).

which is to reduce the time lag behind the transfer of data for criminal investigation. Still, at a minimum, the CSPs should be allowed to communicate to the UK and the U.S. governments regarding the extent to which U.S. persons' data is integrated with that of the targeted person.

Additionally, the language in the CLOUD Act may be amended to permit the CSPs to object to judicial orders of QFGs by adopting similar provisions regarding the requirements of Motion to Modify or Quash in the United States. This way, in the United Kingdom, for example, a CSP could object to UK court orders if it reasonably believes that the targeted person is not a UK citizen, does not reside in the United Kingdom, and if the disclosure would violate US laws. Thus, the Fourth Amendment will come into play. The UK authorities would be forced to use caution when requesting certain data from the CSPs in order to avoid invoking any objections, which comes with the risk of delaying the investigation process. This will permit the CSPs with more avenues to take an active role in protecting the consumer data from unlawful disclosure by effectively enforcing the probable cause standard.

CONCLUSION

The CLOUD Act, as part of a larger omnibus bill, was passed within three-weeks after the Supreme Court heard the arguments from the parties in *Microsoft*. In doing so, Congress implied that protecting privacy comes second to expediting criminal investigations processes. This is further supported by the fact that the United Kingdom is the first country to have entered into an executive agreement, given the strength of UK laws' protection for privacy, or rather, lack thereof.

To protect the privacy of the U.S. citizens while also fulfilling the primary purpose behind the CLOUD Act, clarifying clear standards to be applied in evaluating a foreign government's candidacy is essential. Alternatively, an independent authority may be created to provide input in determining whether a prospective foreign government satisfies the elements laid out in the CLOUD Act. Furthermore, legislative actions can create additional avenues for relief to U.S. citizens whose privacy has been breached. Lastly, the CSPs can also play an active role in protecting consumer data by

requiring them to implement similar notification procedures and providing specific grounds for them to object to a QFG's request for data.

Looking forward, without additional safeguards discussed here, the European country's arguably less robust privacy laws may become the new standard to be met by other potential QFGs. In other words, another foreign country with a minimal data protection regime may qualify for an executive agreement as long as its privacy laws is as strong as those of the United Kingdom. This does not seem to be a high bar, taking into consideration the EU's refusal to declare that the country is eligible for an Adequacy Decision "by default" upon its exit from the bloc. [234] This implies that even the EU cannot confidently say that the UK data protection laws as they stand currently meets the higher standards set by the GDPR. If the UK privacy laws become the norm, the United States may be further behind its competitors as other countries introduce increasingly robust privacy laws to attract businesses and gain market share in the digital economy.

To be sure, the primary purpose of the CLOUD Act, which is to smooth the cross-border data transfer for criminal investigation purposes, is noble and crucial, especially today when the rate at which the digital economy is growing overwhelmingly outpaces that of its regulations. As of this writing, the Congressional review period required under the CLOUD Act of the Executive Agreement

[234] *UK sent "chilling" warning over EU Adequacy Decision*, GDPR ASSOCIATES (Jan. 16, 2018), https://www.gdpr.associates/uk-sent-chilling-warning-eu-adequacy-decision/; *see also* Cameron Abbott, *Post-Brexit Data Protection – Where Are We Now?*, THE NAT'L. L. REV. (Feb. 4, 2020) https://www.natlawreview.com/article/post-brexit-data-protection-where-are-we-now; David Cowan, *GDPR Regime Emerges as Early Candidate for Post-Brexit Divergence*, THE GLOB. LEGAL POST (Feb. 4, 2020) http://www.globallegalpost.com/big-stories/gdpr-regime-emerges-as-early-candidate-for-post-brexit-divergence-460121/ (reporting that the United Kingdom's Foreign Secretary Dominic Raab said that the country will "not be aligning with EU rules.").

has not lapsed yet.[235] While there is little doubt that Executive Agreement will go unchallenged by the Legislature, this Article identifies potential problems regarding data privacy that should be considered regardless of whether the Executive Agreement is approved or not. To be clear, the problems identified in this Article are only the tip, if that, of myriad issues and uncertainties surrounding cross-border data transfer. At the minimum, this Article emphasizes that it is difficult to balance the importance of data privacy and that of criminal prosecutions. But this balancing must be taken with careful consideration and scrutiny when implementing a new data protection regime today.

[235] On January 16, 2020, Assistant Attorney General Stephen E. Boyd sent a letter to Congress stating that, while the Executive Agreement was entered into in October 2019, because the Department of Justice failed to notify the Congress until January 10, 2020 due to "clerical error . . . [DOJ] considers July 8, 2020 to be the date upon which the agreement will enter into force, absent the enactment into law of a resolution of disapproval as set forth under [18 U.S.C. § 2523(b)]." Supplementary Letter from Assistant Att'y Gen. Stephen E. Boyd to U.S. Congress in Support of U.S.-U.K. CLOUD Act Agreement, U.S. DEP'T OF JUST. (Jan. 16, 2020), https://www.justice.gov/dag/page/file/1236281/download.